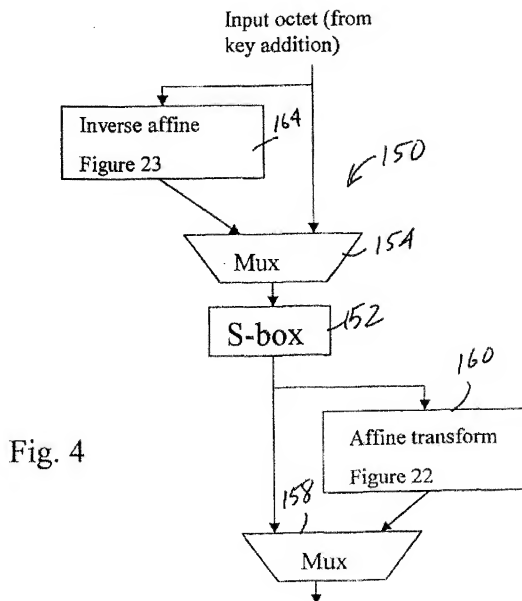## Remarks

In the non-final Office Action dated August 13, 2009, the following new grounds of rejection are presented: claims 1-2, 4-5, 8-10, 12-15 and 18 stand rejected under 35 U.S.C. § 102(b) over Van Buer (U.S. Patent Pub. 2003/0198345); and claims 6-7, 11 and 16-17 stand rejected under 35 U.S.C. § 103(a) over the '345 reference in view of Dent (U.S. Patent No. 5,091,942). Claim 3 is objected to as being dependent upon a rejected base claim but would be allowable if rewritten in independent form. The Office Action notes that Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date under 35 U.S.C. § 119(e). Applicant addresses these rejections in the following discussion which does not acquiesce in any regard to averments in this Office Action (unless Applicant expressly indicates otherwise).

Applicant appreciates the indicated allowability of claim 3, if written in independent form.

Applicant respectfully traverses the § 102(b) and § 103(a) rejections of claims 1-2 and 4-18 because the cited '345 reference either alone or in combination with the '942 reference lacks correspondence to the claimed invention. For example, neither of the asserted references teaches the claimed invention "as a whole" (§ 103(a)) including aspects regarding, *e.g.,* a circuit configured to perform an affine-all transformation that performs both an affine and inverse affine transformation.

More specifically, Applicant's affine-all transformation reduces the pair of affine transform and inverse affine transform to one transform (*e.g.,* a single affine transform as recited in claims 12 and 14). Applicant's specification teaches that this aspect can be particularly useful in that an affine-all transformation circuit can perform both the normal and inverse affine transformations with very little duplicate logic as discussed, for example, in paragraph 0019 of the published version of Applicant's specification (*see also* claim 4 which recites "a circuit having shared logic that performs a single transform that accomplishes an affine and an inverse affine transformation"). The '345 reference, however, does not teach an affine-all transformation as in the claimed invention, but instead discloses that separate logic is used to perform an inverse affine transform 164 and an affine transform 160 as is shown in FIG. 4 as reproduced below. *See also* paragraph 0068.

Input octet (from
key addition)

Inverse affine

Figure 23

164

150

Mux

154

S-box

152

160

Affine transform

Figure 22

158

Mux

Fig. 4

The '345 reference further illustrates the separate logic that implements the
inverse affine transform in FIG. 5 and the affine transform in FIG. 6. Instead of teaching
an affine-all transform, the '345 reference expressly teaches away from combining of
such aspects, *e.g.*, "keeping most of the logic for encryption and decryption separate can
reduce the amount of multiplexing needed to combine alternate logic" and that "(s)uch a
design can use two nearly independent pipelines that only share the S-boxes." Paragraph
0082. As such, the '345 reference does not teach an affine-all transformation that
performs both affine and inverse affine transforms as a single transformation, as in the

claimed invention. Thus, the '345 reference does not provide correspondence to the claimed invention.

Moreover, the Office Action's apparent assertion that the separate affine and inverse affine transformations taught by the '345 reference correspond to Applicant's all-affine transformation is improper because such an interpretation of an all-affine transformation is inconsistent with Applicant's specification as discussed, for example, in paragraphs 0018 and 0019 of the published version of the instant application. Thus, the Office Action's apparent interpretation of an all-affine transformation violates M.P.E.P. § 2111.

In addition, the '345 reference does not teach an affine-all transformation that performs both an affine and inverse affine transformation in response to respective load patterns, as recited in claim 1. The Office Action does not appear to address aspects of the claimed invention relating to respective load patterns as no mention is made of these aspects in the instant Office Action. Moreover, Applicant submits that the '345 reference does not teach that the separate affine and inverse affine transforms that are performed by blocks 160 and 164 are in response to any load patterns. Instead, the '345 reference teaches that each of blocks 160 and 164 performs a single affine or inverse affine transform. This function is performed regardless of any input as shown in more detail in FIGs. 5-6.

Furthermore, the Office Action fails to address claims 12 and 13 under § 112(6) as required by M.P.E.P. § 2181 ("the PTO may not disregard the structure disclosed in the specification corresponding to such language when rendering a patentability determination"). As the required § 112(6) analysis has been undertaken there is not a *prima facie* case for the rejection. For instance, the Examiner has disregarded the structure disclosed in Applicant's specification (*see, e.g.,* FIG. 4) with regard to the claimed means for performing an affine-all transform. As such, the rejection cannot stand and should be withdrawn.

With specific regard to the rejection under § 103(a), the proposed modification in view of the '942 reference does not cure the above-mentioned deficiencies and is therefore also improper.

In view of the above, the § 102(b) and § 103(a) rejections are improper and Applicant requests that they be withdrawn.

8

Applicant has also added new claim 19, which depends from claim 4 and, thus, is allowable over the cited references for at least the reasons discussed above. Applicant notes that support for claim 19 can be found throughout Applicant's disclosure including, for example, in paragraphs 0025-0027 of the published version of the instant application.

In view of the remarks above, Applicant believes that each of the rejections has been overcome and the application is in condition for allowance. Should there be any remaining issues that could be readily addressed over the telephone, the Examiner is asked to contact the agent overseeing the application file, Juergen Krause-Polstorff, of NXP Corporation at (408) 474-9062 (or the undersigned).

Please direct all correspondence to:

Corporate Patent Counsel
NXP Intellectual Property & Standards
1109 McKay Drive; Mail Stop SJ41
San Jose, CA 95131

CUSTOMER NO. 65913

By: _____
Name: Robert J. Crawford
Reg. No.: 32,122
Name: Shane O. Sondreal
Reg. No.: 60,145
651-686-6633
(NXPS.604PA)